PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00	A1	(11) International Publication Number: WO 98/27685
		(43) International Publication Date: 25 June 1998 (25.06.98)

(21) International Application Number: PCT/US97/21900

(22) International Filing Date: 25 November 1997 (25.11.97)

(30) Priority Data:
08/768,674 18 December 1996 (18.12.96) US

(71) Applicant: INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

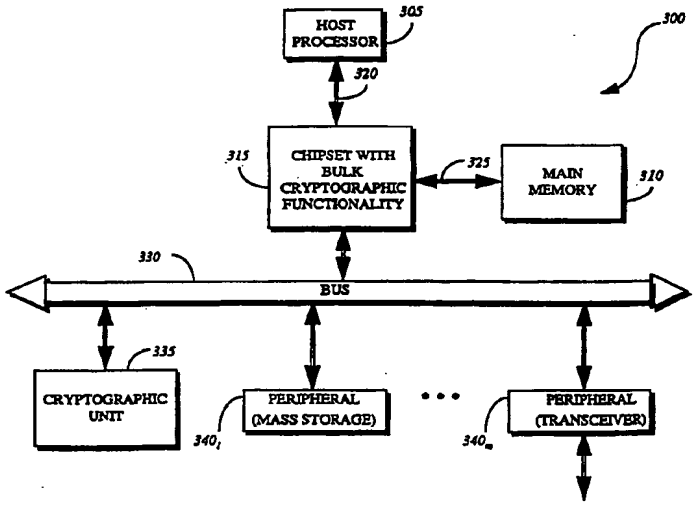
(72) Inventor: DAVIS, Derek, L.; 4509 East Desert Trumpet Road, Phoenix, AZ 85044 (US).

(74) Agents: TAYLOR, Edwin, H. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025-1026 (US).

(81) Designated States: AL, AM, AT, AT (Utility model), AU (Petty patent), AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: OPTIMIZED SECURITY FUNCTIONALITY IN AN ELECTRONIC SYSTEM



(57) Abstract

The electronic system (300) includes a host processor (305), a chipset with bulk cryptographic functionality (315), a main memory (310), and a cryptographic unit (335). The electronic system (300) also includes a host bus (320), a memory bus (325), and a bus (330). The cryptographic unit (335) includes circuitry to control and to manage bulk cryptographic operations that are performed by the chipset (315) using secret keys and/or session keys in the cryptographic processing performed.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

OPTIMIZED SECURITY FUNCTIONALITY IN AN ELECTRONIC SYSTEM

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the field of cryptography. More particularly, the present invention relates to an electronic system that includes security functionality to optimize performance of the electronic system during cryptographic operations.

2. Description of Art Related to the Invention

In today's society, it is becoming necessary to protect information transmitted from a personal computer ("PC") so that the information is clear and unambiguous to an authorized receiver, but incomprehensible to any unauthorized persons. Additionally, it is becoming necessary to protect information stored within the PC to prevent unauthorized persons from downloading information onto a floppy disk, digital tape or other type of content storage device. Protection against unauthorized downloading may be accomplished by placing the information in an encrypted format prior to storage within the PC. Such encryption may be performed by either (i) a processing unit of the PC executing cryptographic software, or (ii) a cryptographic device solely connected to a system bus of the PC.

Referring to Figure 1, the PC 100 designed in accordance with a conventional cryptographic implementation scheme is shown. The PC 100 includes a host processor 105 coupled to a chipset 110. The chipset 110 operates as a communicative pathway to both main memory 115 and an internal bus 120. A number of peripheral devices may be coupled to the

internal bus 120 including a Personal Computer ("PC") card 125 that is used in this embodiment to provide cryptographic functionality to PC 100. Other peripheral devices include a parallel port device 126, a modem 127, and a disk controller 128 being an interface to a storage device such as a hard disk drive ("HDD") 129. This conventional architectural scheme may simplify the implementation of cryptographic functionality into an existing PC platform without an appreciable effect on various components already implemented therein; however, it adversely impacts performance of PC 100.

More specifically, a primary disadvantage associated with the conventional cryptographic implementation of Figure 1 is that a cryptographic device 130, solely implemented within the PC 100 as a peripheral device such as a PC card, would adversely affect bandwidth of internal bus 120. The reason for the adverse effect is that performance of "bulk cryptographic operations" would require data to be transferred through internal bus 120 a multiple number of times. "Bulk cryptographic operations" are defined as operations involving (i) cryptography that supports high-volume throughput, (ii) hashing and the like. The cryptography utilized by bulk cryptographic operations typically involves symmetric key cryptography (e.g., encryption or decryption under Data Encryption Standard "DES" and other functions), or perhaps may involve asymmetric key cryptography.

For example, in order to store data in an encrypted format within a peripheral device such as HDD 129, the data residing in main memory 115 and having a non-encrypted format would be initially transferred to the peripheral device containing cryptographic device 130. Thereafter, cryptographic device 130 would encrypt the data and either transfer the encrypted data to HDD 129 or to main memory 115 for subsequent transmission to HDD 129. In either scenario, the data propagates through internal bus 120 at least two and perhaps three times, in contrast to the

normal propagation of data directly from main memory 115 to HDD 129 in those cases when data is being stored in a non-encrypted format.

Referring now to Figure 2, another embodiment of a PC 200, designed in accordance with a second conventional cryptographic implementation scheme, is shown. The PC 200 includes a host processor 205 coupled to a chipset 210, main memory 215 and an internal bus 220 as described above. Contrary to the conventional cryptographic implementation scheme of Figure 1 in which cryptography is performed by the cryptographic device acting as a separate peripheral device, cryptographic circuitry is implemented into each of the peripheral devices 225_1-225_n ("n" being a positive whole number) connected to internal bus 220. This embodiment would avoid unacceptable bus bandwidth latency, but would impose other disadvantages. One disadvantage is that this embodiment increases the costs of each peripheral device 225_1-225_n. Typically, these additional costs result from greater component costs due to increased circuitry and greater design and manufacturing costs. Another disadvantage that may occur is that this embodiment increases the likelihood of future compatibility problems as different cryptographic circuitry enters the marketplace.

Thus, it would be desirable to develop a system and method of operation that overcomes the above-described disadvantages.

SUMMARY OF THE INVENTION

The present invention relates to an electronic system having security functionality that optimizes performance of the electronic system during cryptographic operations. The electronic system includes a chipset implemented with dedicated circuitry to perform bulk cryptographic operations. The cryptographic operation of the chipset may be controlled and managed by circuitry physically removed from the chipset, and in secure communications therewith, such as the host processor or a

cryptographic unit. The cryptographic operation of the chipset may also be controlled and managed by circuitry of the chipset.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is a conventional PC platform providing cryptographic functionality through a cryptographic device having a dedicated connection to an internal bus.

Figure 2 is a conventional PC platform providing cryptographic functionality by implementing cryptographic devices into peripherals coupled to the internal bus.

Figure 3 is an embodiment of an electronic system providing improved performance during cryptographic operations by implementing partitioned secure cryptographic functionality in which bulk cryptographic operations are performed by the chipset which are controlled and managed by a separate cryptographic unit.

Figure 4 is a more-detailed embodiment of the chipset and the cryptographic unit.

Figure 5 is an illustrative block diagram of the session key storage element.

Figure 6 is another embodiment of an electronic system providing improved performance during cryptographic operations by implementing partitioned secure cryptographic functionality in which bulk cryptographic operations are performed by the chipset which are controlled and managed by the host processor.

Figure 7 is an illustrative flowchart of the general cryptographic operations performed by both the chipset and either the cryptographic unit or host processor in decrypting information obtained from a remote source.

Figure 8 is an illustrative flowchart of cryptographic operations performed by both the chipset and either the cryptographic unit or host processor in encrypting information contained in main memory for storage within the electronic system.

Figure 9 is yet another embodiment optimizing system performance during cryptographic operations by implementing cryptographic circuitry onto the chipset.

Figure 10 is a more-detailed embodiment of the chipset of Figure 9.

DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention relates to an electronic system and method for optimizing system performance during cryptographic operations. In the following description, some terminology is used to discuss certain well-known cryptographic functions. For example, an "electronic system" is a system including processing and internal data storage which may include, but is not limited to a computer such as laptops or desktops, servers, imaging devices (e.g., printers, facsimile machines, scanners, etc.), financial devices (e.g., ATM machines) and the like. "Information" is defined as one or more bits of data, address, and/or control. A "message" is generally defined as information being transferred during one or more bus cycles. A "key" is an encoding and/or decoding parameter used by conventional cryptographic algorithms such as a Data Encryption Algorithm as specified in Data Encryption Standard ("DES") and the like. More particularly, a "session key" is a temporary key used in connection with symmetric cryptography to provide secure communications. A "digital signature" is a message typically used for authentication purposes.

The term "secure" indicates that it is virtually computationally infeasible for an unauthorized individual to access information in a non-encrypted format or to successfully perpetuate fraud by tampering with such information.

Referring to Figure 3, an illustrative embodiment of an electronic system 300 employing the present invention is shown. The electronic system 300 comprises a host processor 305 and a main memory element 310 (e.g., dynamic random access memory "DRAM", static random access memory "SRAM", etc.) coupled together by a chipset 315. The chipset 315 operates as an interface between a plurality of buses, namely a host bus 320, a memory bus 325 and bus 330. Besides logic used to perform its standard functionality of interconnecting multiple buses, which is not discussed in detail to avoid obscuring the present invention, the chipset 315 may require modification to include dedicated circuitry that performs bulk cryptographic operations on messages transferred through chipset 315. Such dedicated circuitry is included within the chipset, regardless of whether it is physically located within an integrated circuit package of the chipset or outside the chipset's package but coupled to both the chipset 315 and bus 330. An illustrative embodiment of such circuitry is shown in Figure 4.

Referring still to Figure 3, the bus 330 provides a communication path between (i) a cryptographic unit 335 and (ii) a plurality of peripheral devices 340_1-340_m ("m" being a positive whole number). The bus 330 may be a Peripheral Component Interconnect ("PCI") bus, Industry Standard Architecture ("ISA") bus or any other type of bus architecture. It is contemplated that bus 330 is shown as a single bus (e.g., the PCI bus), but it may be multiple buses coupled together through bridge circuitry in which each peripheral device 340_1-340_m is coupled to at least one of the multiple buses.

The cryptographic unit 335 includes circuitry to control and manage bulk cryptographic operations performed by the chipset 315. This is accomplished through the use of secret and/or session keys to establish secure communications with the chipset 315. Additionally, peripheral devices 340_1-340_m may include, but are not limited to, a mass storage device 340_1 (e.g., a hard disk drive, a CD ROM player, CD recordable player, digital tape drive, a floppy disk drive, a digital video disk player, etc.), a transceiver device 340_m (e.g., a network interface circuit card, a modem card, etc.) and the like.

Referring now to Figure 4, illustrative embodiments of chipset 315 and cryptographic unit 335 are shown. The chipset 315 includes circuitry 400 that performs bulk cryptographic operations on digital information propagating through the electronic system. The circuitry 400 includes a cryptographic engine 405 coupled to bus 330 and memory bus 325, a session key storage element 410 and a secret key storage element 420. The cryptographic engine 405 may possess a unique communication path to main memory via memory bus 325 or share this communication path with other circuitry through conventional multiplex hardware. The session key storage element 410 and the secret key storage element 420 are coupled to cryptographic engine 405 through signal lines 415 and 425, respectively. The signal lines 415 and 425 may have the same or different bit widths, ranging from one-bit to r-bits ("r" being a positive whole number, $r > 1$).

The cryptographic engine 405 is circuitry (e.g., hardware or firmware) that performs a bulk cryptographic operation on input data based on a key supplied by either the session key storage element 410 or secret key storage element 420, or based on a hash function if hashing is performed. The session key storage element 410 is used to store session keys that are used when performing bulk cryptographic operations on data input into the cryptographic engine 405. More specifically, these bulk

cryptographic operations may use the session key to decrypt data transferred to main memory from one of the peripheral devices or to encrypt data transferred to one of the peripheral devices for storage or transmission. Such encryption or decryption may be performed through Data Encryption Algorithm or other symmetric cryptographic functions, while hashing may be performed through cryptographic hash functions such as Message Digest 5 ("MD5") provided by RSA Data Security of Redwood City, California, Secure Hash Algorithm ("SHA-1") specified by the National Institute of Standards and Technology of Washington, D.C., and other established hash functions.

Typically, the session key storage element 410 is implemented with volatile memory to contain one or more session key(s). In one embodiment, the session key storage element 410 may be configured as cache memory that supports one or more session keys although such caching architecture is not required. As generally shown in Figure 5, one embodiment of the session key storage element 410 includes multiple storage entries 500_1-500_X ("x" being a positive whole number), accessible by bus lines coupled thereto (not shown). Each storage entry 500_1-500_X pertains to one unique key and provides sufficient storage to support at least three fields associated with that key; namely, a session key field ("SKF") 505_1-505_X, a priority/validity field ("PVF") 510_1-510_X and at least one address information field ("AIF") 515_1-515_X. The session key field 505_1-505_X is used to contain different session keys used when performing bulk cryptographic operations. The priority/validity field 510_1-510_X is used to identify an "invalid" entry and to establish a priority in determining which entries may be overwritten when loading new session keys. The address information field(s) 515_1-515_X include information relating to the source and destination addresses of a message being processed.

Referring back to Figure 4, cryptographic unit 335 is used to control and manage bulk cryptographic operations performed by the chipset 315 as well as to support a secure communication path and interconnection with the chipset 315 and possibly other systems. The cryptographic unit comprises a bus 600 interconnecting a processing unit 605, non-volatile memory element 610, an optional volatile memory element 615 (as denoted by dashed lines), and an optional random number generator ("RNG") 620 (as denoted by dashed lines). The processing unit 605 may include, but is not limited to a processor, a micro-controller, a state machine logic circuit and the like. The non-volatile memory element 610 contains at least a shared secret key, which is also imprinted into the secret key storage element 420 normally during manufacture when the cryptographic unit 335 and the chipset are powered up and in communication with each other. This imprinting may be performed by an original equipment manufacturer ("OEM") of the electronic system, suppliers of the chipset and/or cryptographic unit, or a specified third party.

The shared secret key is generated by random number generator 620, if implemented, or an externally available random number generator. It is contemplated that the shared secret key may be produced after manufacture by an OEM or a trusted authority (e.g., trade association, governmental entity or other "trusted" entity). As discussed, the shared secret key may be used by both chipset 315 and cryptographic unit 335 to encrypt and decrypt information or to establish a "session" key used for that purpose. It is further contemplated that volatile memory element 615, if implemented, may be utilized as temporary storage by the processing unit 605.

Referring to Figure 6, another embodiment of the electronic system providing improved performance during cryptographic operations is shown. The electronic system is similar to that shown in Figure 3 with the exception that no cryptographic unit is implemented to control and manage

the chipset. Rather, it is contemplated that the host processor may control and manage the performance of bulk cryptographic operations by the chipset 315 through a combination of software and hardware.

Referring now to Figure 7, a flowchart illustrating the operations of an electronic system, implemented with partitioned data security functionality, to decrypt a message in an encrypted format received by a transceiver of the electronic system is shown. Upon receiving an encrypted message, a header of the message is transferred to the cryptographic unit (Step 705). The header includes a session key (hereinafter referred to as a "mail key") encrypted with other information. The mail key is extracted from the header of the message by decrypting the header with a key contained in memory of the cryptographic unit (Step 710). The key may be a private key associated with the electronic system if public/private key cryptography is used to secure communications between the electronic system and other networked systems. In the case that the host processor is performing the functions of the cryptographic unit in controlling the bulk cryptographic operations of the chipset, the header is processed by the host processor using a key to which the host processor has access.

Next, the mail key is securely transmitted to the chipset, destined for the session key storage element (Step 715). This secure transmission is accomplished by the cryptographic unit or host processor producing a control message being the mail key encrypted under a message key. The "message key" is either the shared secret key or a session key established through the use of the shared secret key. The control message can be transmitted to the chipset, which decrypts the control message, using the message key, to recover the mail key. Subsequently, the mail key is loaded into the session key storage element (Steps 720 and 725). Thereafter, the contents of the message can be transferred through the chipset and decrypted for transmission to main memory.

Referring to Figure 8, a flowchart illustrating the operations of the electronic system, implemented with partitioned data security functionality, to encrypt data before storage in a peripheral device such as HDD, is shown. First, the operating system of the electronic system sends a request to the cryptographic unit (or host processor) requesting preparation to transfer contents of main memory to a hard disk controller (Step 805). The cryptographic unit (or host processor) generates a session key for encryption, referred to as a "file key", and securely transmits the file key to the chipset through the use of the message key (Steps 810 and 815). The chipset places the file key in the session key storage element (Step 820). Thereafter, the OS writes the data contained in main memory to the hard disk controller and the chipset encrypts the data, forming at least a portion of the message, with the file key as it propagates there through. Thus, the data is stored in an encrypted format on HDD (Step 825).

Referring now to Figure 9, it is contemplated that another architectural embodiment of an electronic system 900 employing the present invention may be used, absent partitioned data security functionality as set forth in Figures 3-7. The electronic system 900 includes a chipset 910 performing bulk cryptographic operations and internally controlling these operations. Thus, a dedicated cryptographic unit for control purposes would not be required.

Referring to Figure 10, a more-detailed block diagram illustrating one embodiment of the chipset 910 is shown. Similar to the chipset illustrated in Figure 4, this chipset 910 includes (i) a cryptographic engine 915 coupled to both the bus and the memory bus through internal buses 920 and 925 respectively, and (ii) a session key storage element 930 coupled to the cryptographic engine 915 through a dedicated bus 935. However, chipset 910 further comprises circuitry of controlling and managing the bulk cryptographic operations performed by the cryptographic engine 915. This circuitry includes a processing unit 940

(e.g., a processor, state machine, micro-controller, etc.), coupled to both internal bus 920 and another internal bus 945 coupled to session key storage element 930, and memory capable of storing key information (e.g., public/private key pair or other key information), cryptographic software, or any other data. Preferably, the memory includes a non-volatile memory element 950 coupled to internal bus 945 and/or volatile memory 955. Optionally, as indicated by dashed lines, the chipset 910 may include a random number generator 960, coupled to internal bus 945, to internally produce key information.

In general, chipset 910 differs from chipset 315 of Figures 3-4 in that it is implemented with circuitry and software to control and manage bulk cryptographic operations by the chipset 910 in lieu of external control by the cryptographic unit of Figures 3-4. The advantage of internalizing both the circuitry for performing the bulk cryptographic operations and the circuitry for controlling and managing these operations within the same physical package is that it allows for the elimination of additional storage space for a shared secret key (e.g., the shared key storage element). The reason is that there is lesser need for a cryptographically secure communication because the processing unit is not externally located from the chipset as in partitioned functionality.

For illustrative purposes, the operations of the chipset 910 are discussed in relation to the receipt of an external message (e.g., an electronic mail message). A portion of the external message, namely the header, is transferred from the transceiver to the host processor. Upon the host processor determining that the message is encrypted, it sends the header to the chipset 910. The chipset 910 routes the header to the processing unit 940, which would decrypt the header using key information stored within internal memory of the chipset 910, most likely non-volatile memory element 950. The key information would likely be a private key of the electronic system contained within the chipset 910,

although the key may be a symmetric key if symmetric key cryptography is used.

Upon decrypting the header, the processing unit 940 would extract a mail key from the header and this mail key would be transferred from the processing unit 940 to the session key storage element 930 through internal bus 945. Thereafter, the host processor would arrange the rest of the data forming the external message to be transferred through the cryptographic engine 915 via internal bus 920. The cryptographic engine 915 would decrypt the data of the external message using the mail key, provided by the session key storage element 930 via internal bus 935, and subsequently route the non-encrypted data to main memory via internal bus 925.

While certain exemplary embodiments have been described and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and not restrictive on the broad invention, and that this invention not be limited to the specific constructions and arrangements shown and described, since various other modifications may occur to those ordinarily skilled in the art.

CLAIMS

What is claimed is:

1. A system comprising:
a memory element;
a bus;
a chipset coupled to the bus and the memory element, the chipset including dedicated circuitry to perform a bulk cryptographic operation.

2. The system according to claim 1 further comprising a cryptographic unit coupled to the bus, the cryptographic unit establishes a secure communication with the chipset and provides information to the chipset so that the chipset is able to perform the bulk cryptographic operation.

3. The system according to claim 1 further comprising a host processor coupled to the chipset, the host processor establishes a secure communication with the chipset and provides information to the chipset so that the chipset is able to perform the bulk cryptographic operation.

4. The system according to claim 3, wherein the host processor includes circuitry implemented for controlling the chipset in performing the bulk cryptographic operation.

5. The system according to claim 3, wherein the host processor is executing software to control the chipset in performing the bulk cryptographic operation.

6. The system according to claim 1, wherein the dedicated circuitry is placed within an integrated circuit package of the chipset.

7. The system according to claim 1, wherein the dedicated circuitry is positioned outside the integrated circuit package of the chipset.

8. A system comprising:

memory means for storing information;

bus means for transferring the information; and

circuit means for performing a bulk cryptographic operation on the information, said circuit means being directly connected to the memory means and the bus means.

9. A system comprising:

a bus;

a chipset coupled to the bus, the chipset including dedicated circuitry to perform a bulk cryptographic operation; and

a cryptographic unit coupled to the bus, the cryptographic unit establishes a secure communication with the chipset and provides information to the chipset so that the chipset is able to perform the bulk cryptographic operation.

10. The system according to claim 9, wherein the cryptographic unit includes

an internal bus;

a processing unit coupled to the internal bus; and

a non-volatile memory element coupled to the internal bus, the non-volatile memory element capable of storing at least a secret key.

11. The system according to claim 10, wherein the cryptographic unit further includes a random number generator which, when activated by the processing unit, generates the secret key subsequently loaded into the non-volatile memory element.

12. The system according to claim 10, wherein the non-volatile memory element of the cryptographic unit further capable of storing a private key associated with the system to support public-private key cryptography with another system.

13. The system according to claim 11, wherein the cryptographic unit further includes a volatile memory element coupled to the internal bus.

14. The system according to claim 10, wherein the dedicated circuitry of the chipset includes

a cryptographic engine coupled to the bus; and

a first storage element coupled to the cryptographic engine, the first storage element capable of containing at least the secret key.

15. The system according to claim 14, wherein the dedicated circuitry of the chipset further includes a second storage element coupled to the cryptographic engine, the second storage element capable of containing at least one session key produced by the cryptographic unit for use by the chipset during the bulk cryptographic operation.

16. The system according to claim 15, wherein the second storage element operates as cache memory including a plurality of storage

entries, each storage entry capable of containing a session key, addressing information, and priority/validity information pertaining to the session key.

17. The system according to claim 14, wherein the cryptographic engine is performing one of (i) cryptographic operations on incoming data into the chipset, and (ii) hashing operations on the incoming data.

18. An electronic system comprising:
processor means for processing data;
means for storing the data in a non-encrypted format;
peripheral means for storing the data in an encrypted format; and
chipset means for interconnecting the memory means to the peripheral means and for performing a bulk cryptographic operation on data input there through by one of the means for storing and peripheral means.

19. The electronic system according to claim 18, wherein the processor means, being coupled to the chipset means, further establishing a secure communication with the chipset means and providing information to the chipset means so that the chipset means is able to perform the bulk cryptographic operation.

20. The electronic system according to claim 18 further comprising cryptographic means for establishing secure communications to the chipset means and for providing information to the chipset means so that the chipset means is able to perform the bulk cryptographic operation.

21. The electronic system according to claim 20, wherein the cryptographic means includes

processing means for processing data;

memory means for storing at least a secret key;

generating means for producing the secret key upon being activated by the processing means; and

internal bus means for interconnecting the processing means, the memory means and the generating means to the chipset means.

22. The electronic system according to claim 21, wherein the generating means includes a random number generator.

23. The electronic system according to claim 21, wherein the memory means includes a non-volatile memory element capable of containing the secret key and a private key of the system to support public-private key cryptography.

24. The electronic system according to claim 21, wherein the chipset means includes

a bus coupled to said cryptographic means and said peripheral means;

a cryptographic engine coupled to the bus; and

a first storage element coupled to the cryptographic engine, the first storage element capable of containing at least a secret key.

25. The electronic system according to claim 18, wherein the chipset means includes

a bus coupled to said cryptographic means and said peripheral means;

a cryptographic engine coupled to the bus; and

a first storage element coupled to the cryptographic engine, the first storage element capable of containing at least a secret key identical to a key contained in the processor means.

26. The electronic system according to claim 24, wherein the chipset means further includes a second storage element coupled to the cryptographic engine, the second storage element capable of containing at least one session key produced by the cryptographic means for use by the chipset means during the bulk cryptographic operation.

27. An electronic system comprising:

a memory element;

a bus;

at least one peripheral device coupled to the bus, the at least one peripheral device including a transceiver to transmit information and to receive information; and

a chipset coupled to the bus and the memory element, the chipset including dedicated circuitry to perform a bulk cryptographic operation.

28. The electronic system according to claim 27 further comprising a cryptographic unit coupled to the bus the cryptographic unit establishes a secure communication with the chipset and provides information to the chipset to enable the chipset to perform the bulk cryptographic operation.

29. The electronic system according to claim 28, wherein the chipset includes

a cryptographic engine coupled to the bus; and

a first storage element coupled to the cryptographic engine, the first storage element capable of containing at least a secret key also imprinted in the cryptographic unit.

30. A method of decrypting data stored in an encrypted format within an electronic system, supporting partitioned cryptographic functionality, including a chipset having dedicated circuitry to perform a bulk cryptographic operation and circuitry to control the chipset, comprising the steps of:

transferring a header of a message to the circuitry;

decrypting the header within the circuitry to obtain a session key;

encrypting the session key with a shared secret key, loaded in both the chipset and the circuitry, to produce a control message;

transferring the control message from the circuitry to the chipset;

decrypting the control message within the chipset using the shared secret key previously loaded in the chipset; and

storing the session key within the chipset for use in performing the bulk cryptographic operation.

31. A method of encrypting data before storage in a mass storage device of an electronic system, supporting partitioned cryptographic functionality, including a chipset having dedicated circuitry to perform a bulk cryptographic operation and circuitry to control the chipset, comprising the steps of:

transferring a request to the circuitry requesting preparation for transfer of data contained in main memory to the mass storage device;

generating a session key internally within the circuitry;

encrypting the session key with a shared secret key previously loaded in both the chipset and the circuitry to produce a control message;

transferring the control message to the chipset;

decrypting the control message with the shared secret key loaded in the chipset;

storing the session key within the chipset; and

encrypting data transferred from the main memory to the mass storage device as the data propagates through the chipset.

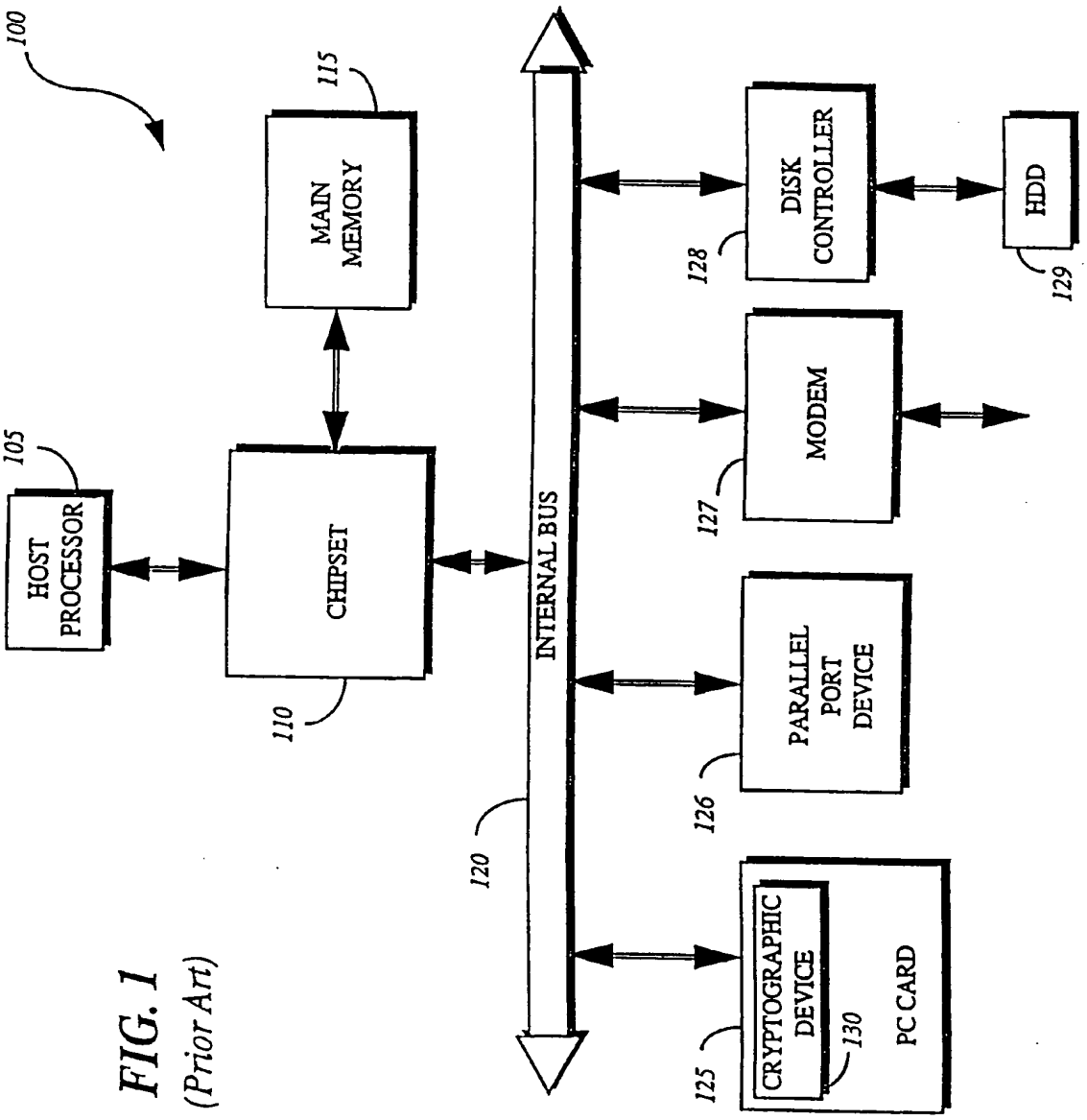


FIG. 1
(Prior Art)

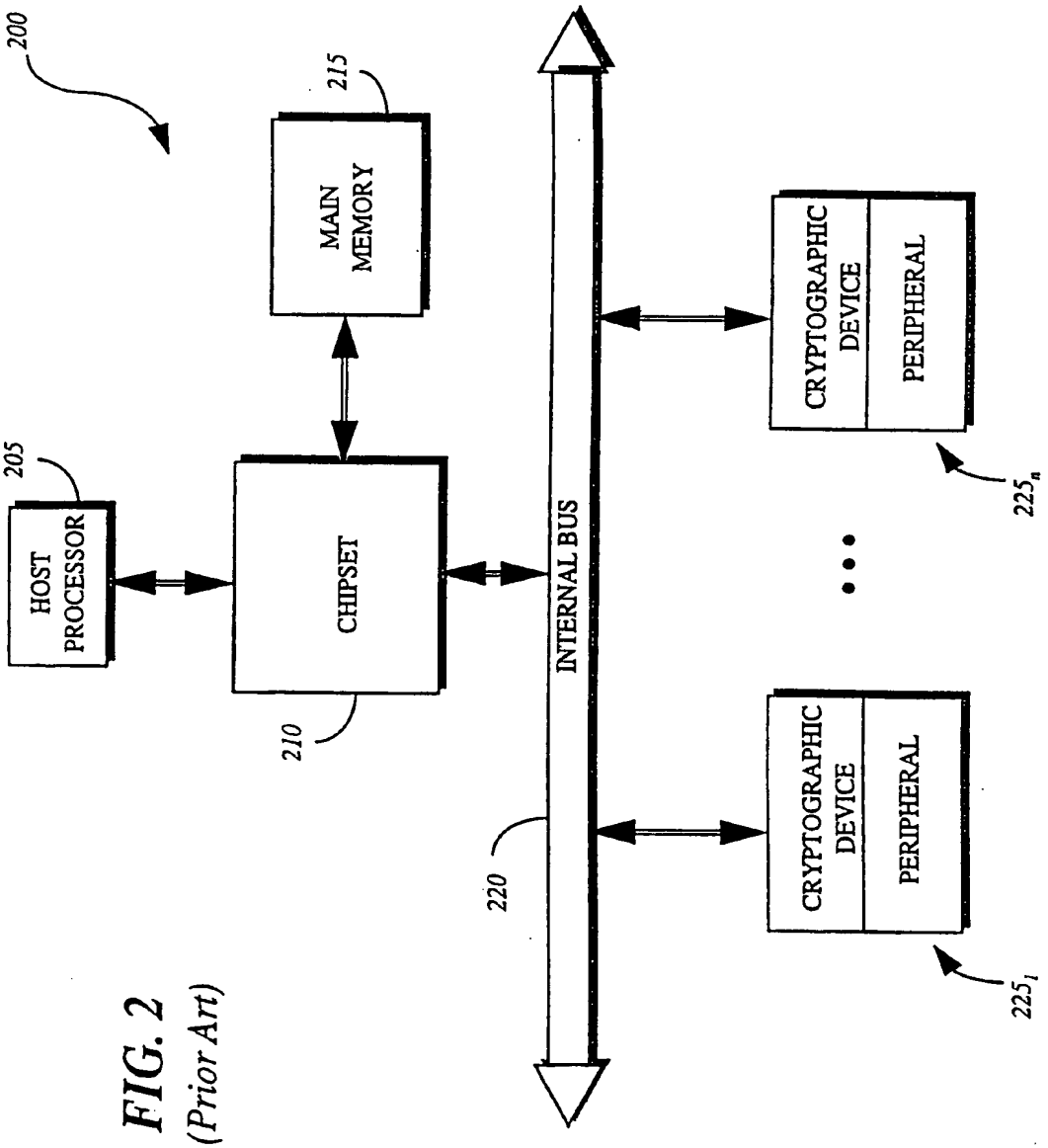


FIG. 2
(Prior Art)

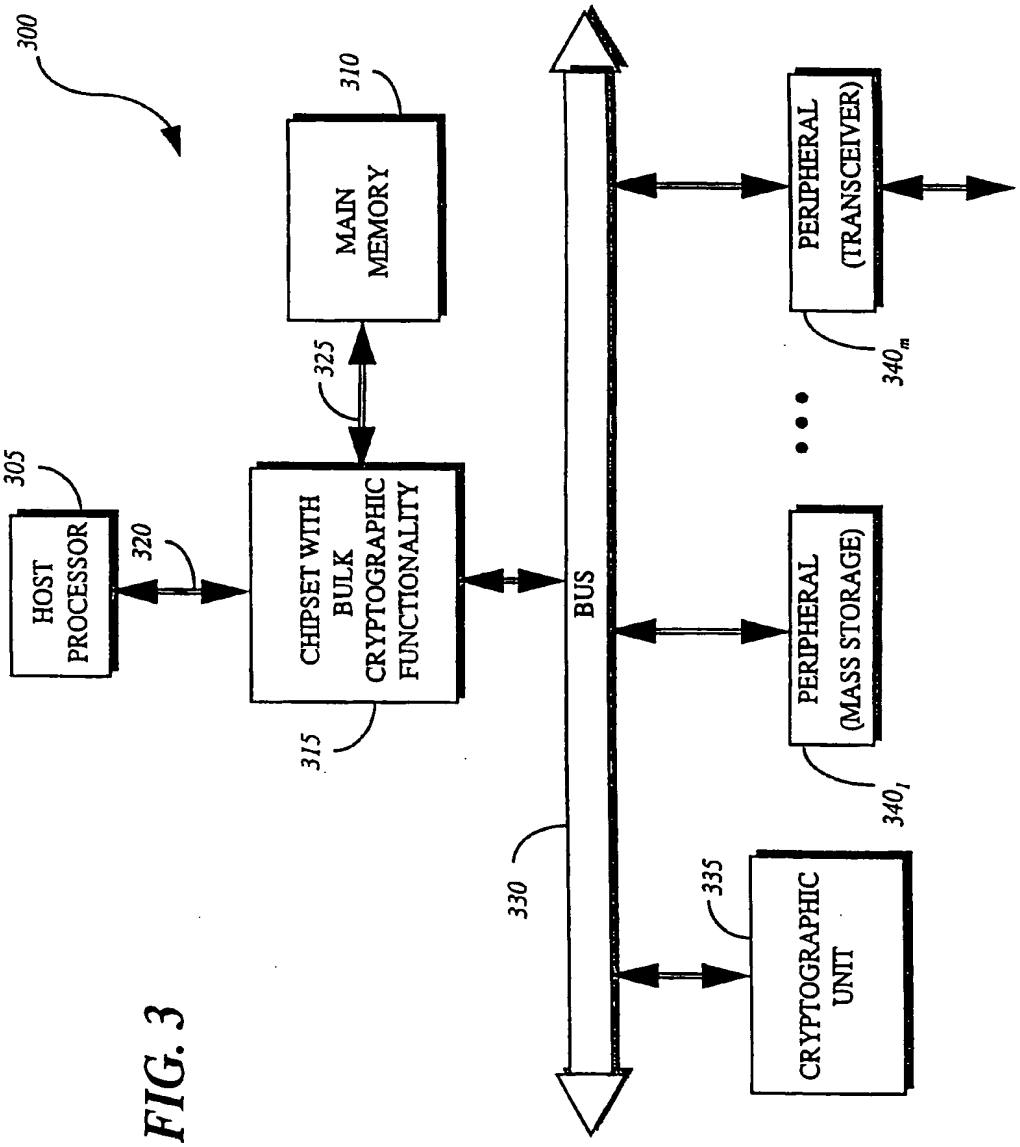

300
310
MAIN MEMORY
325
305
HOST PROCESSOR
320
CHIPSET WITH BULK CRYPTOGRAPHIC FUNCTIONALITY
315
BUS
330
PERIPHERAL (TRANSCEIVER)
340_m
PERIPHERAL (MASS STORAGE)
340_1
335
CRYPTOGRAPHIC UNIT

FIG. 3

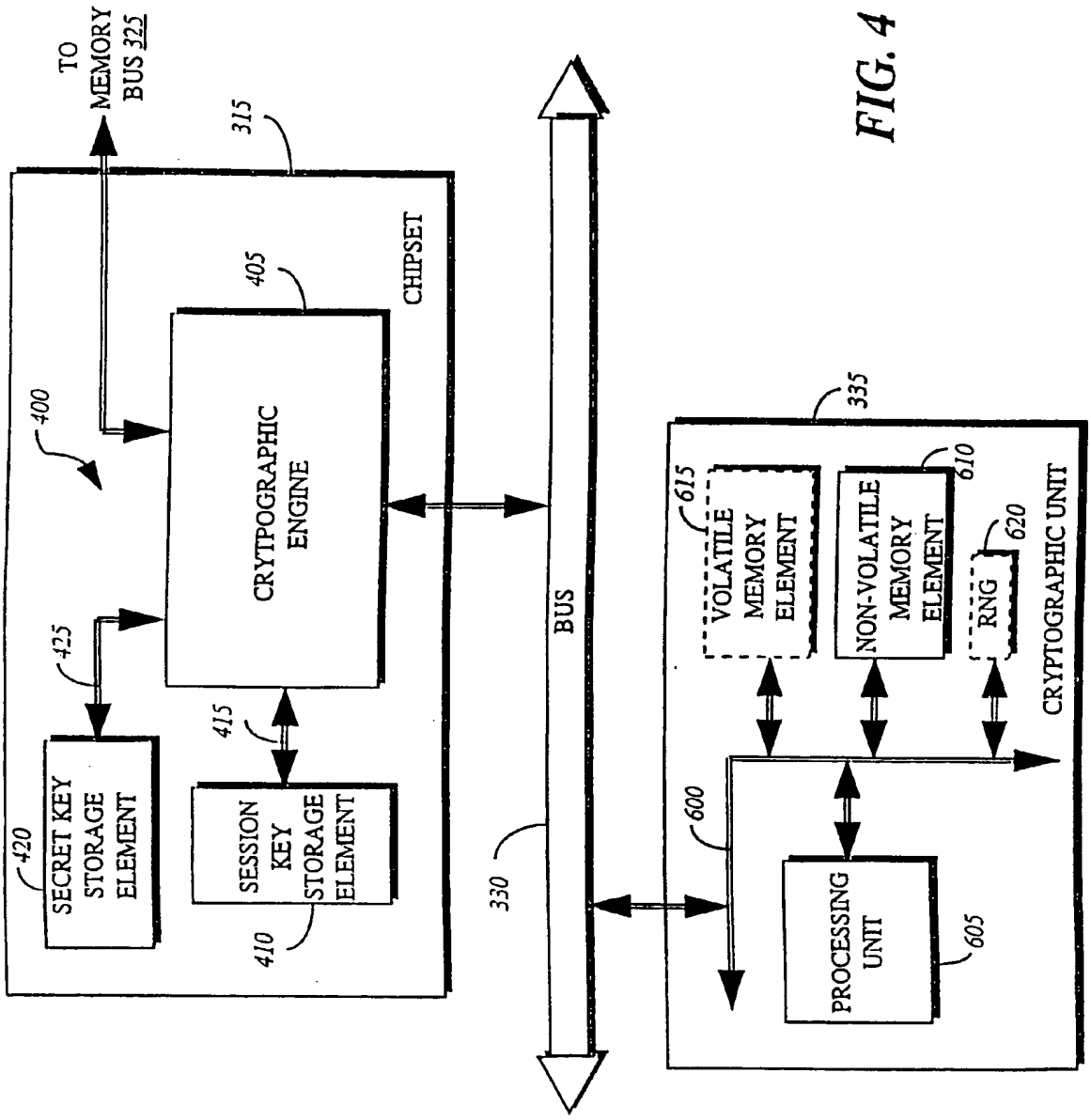

TO MEMORY BUS 325
315
CHIPSET
405
400
CRYTPOGRAPHIC ENGINE
425
415
SECRET KEY STORAGE ELEMENT
420
SESSION KEY STORAGE ELEMENT
410
BUS
330
335
CRYPTOGRAPHIC UNIT
615
VOLATILE MEMORY ELEMENT
610
NON-VOLATILE MEMORY ELEMENT
620
RNG
600
PROCESSING UNIT
605

FIG. 4

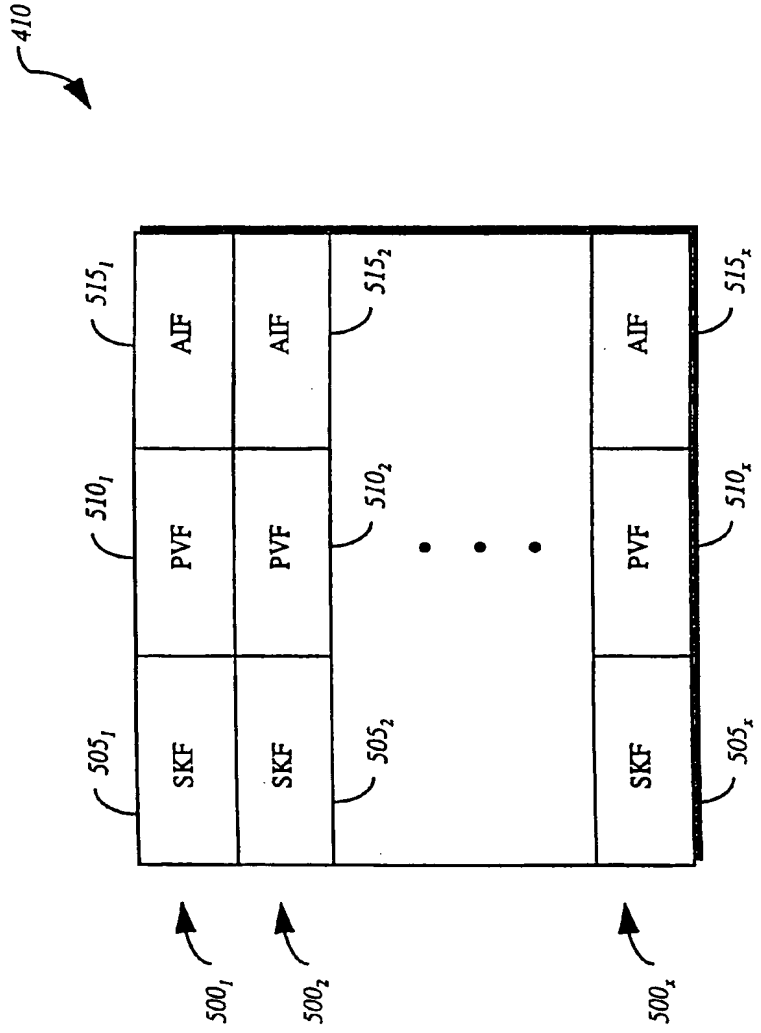

410
AIF
PVF
SKF
515_1
515_2
515_x
510_1
510_2
510_x
505_1
505_2
505_x
500_1
500_2
500_x

FIG. 5

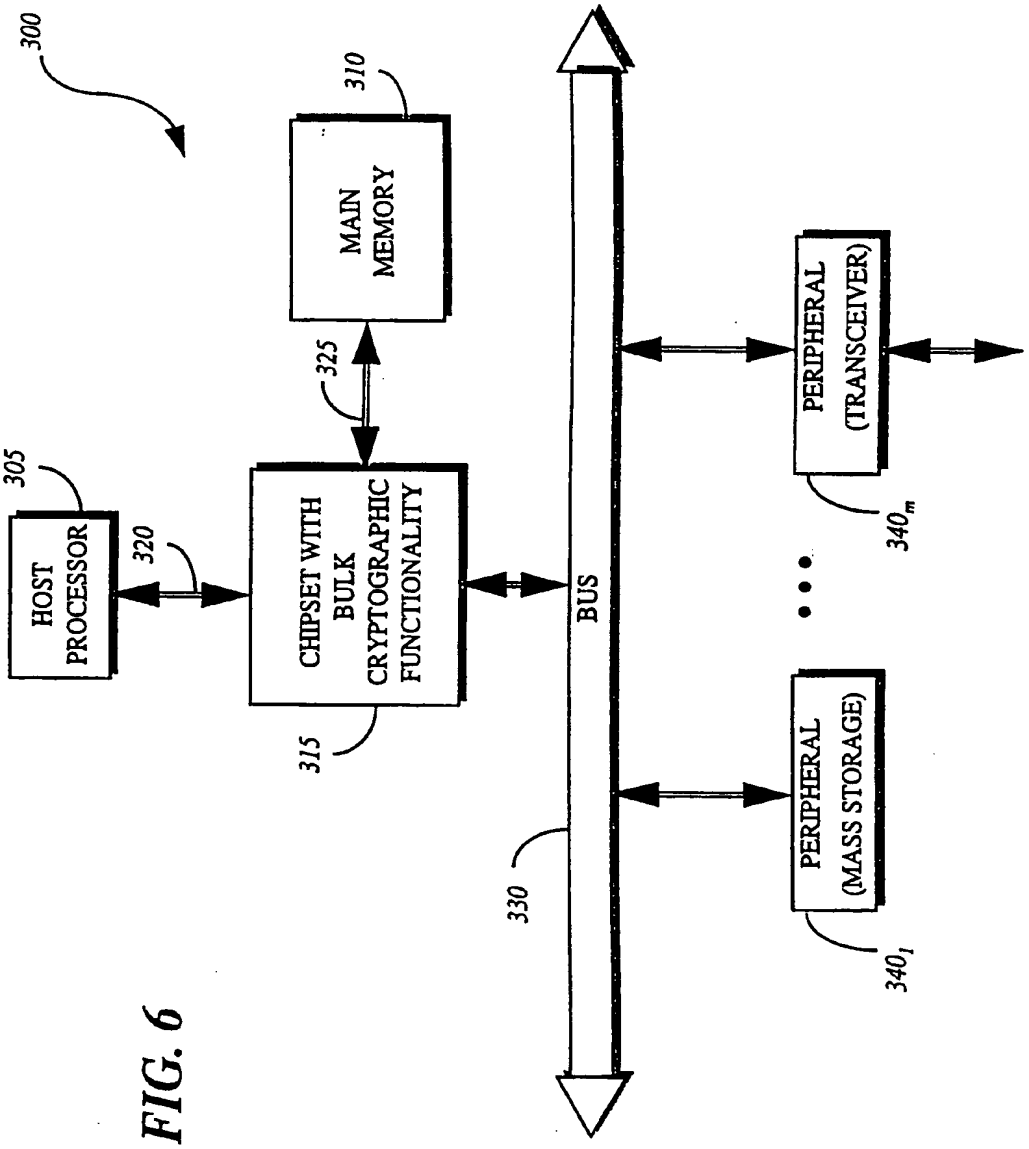

300
310
MAIN MEMORY
325
305
HOST PROCESSOR
320
CHIPSET WITH BULK CRYPTOGRAPHIC FUNCTIONALITY
315
BUS
330
PERIPHERAL (TRANSCEIVER)
340_m
PERIPHERAL (MASS STORAGE)
340_1

FIG. 6

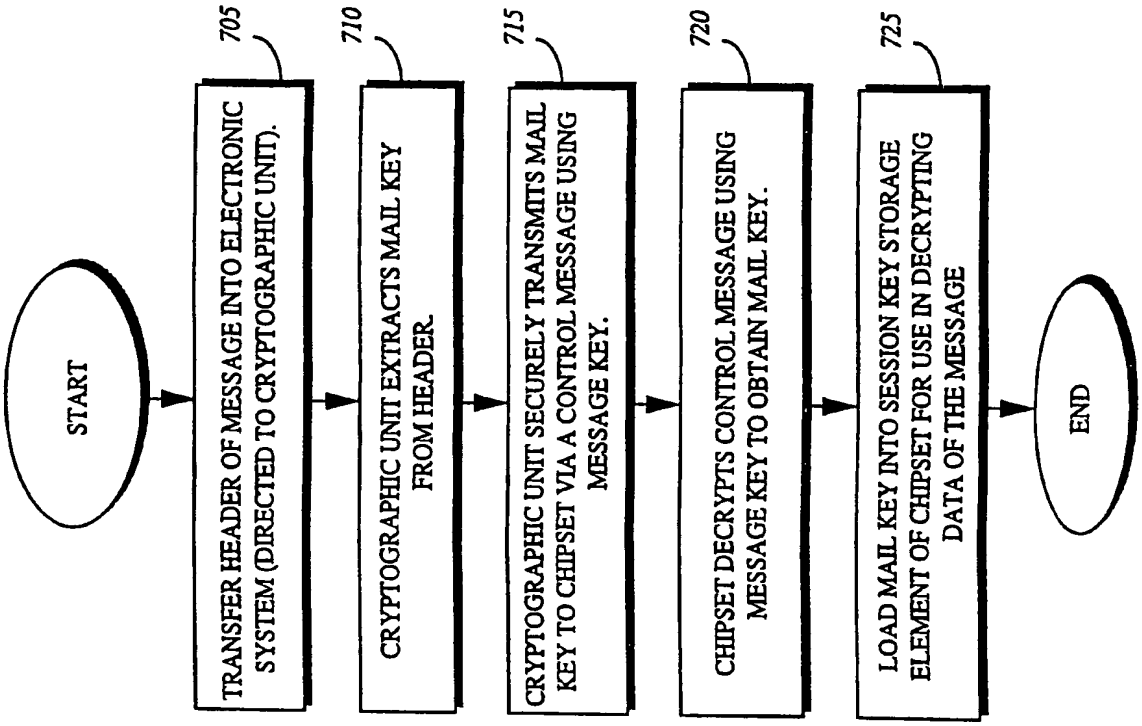

START
705
TRANSFER HEADER OF MESSAGE INTO ELECTRONIC SYSTEM (DIRECTED TO CRYPTOGRAPHIC UNIT).
710
CRYPTOGRAPHIC UNIT EXTRACTS MAIL KEY FROM HEADER.
715
CRYPTOGRAPHIC UNIT SECURELY TRANSMITS MAIL KEY TO CHIPSET VIA A CONTROL MESSAGE USING MESSAGE KEY.
720
CHIPSET DECRYPTS CONTROL MESSAGE USING MESSAGE KEY TO OBTAIN MAIL KEY.
725
LOAD MAIL KEY INTO SESSION KEY STORAGE ELEMENT OF CHIPSET FOR USE IN DECRYPTING DATA OF THE MESSAGE
END

FIG. 7

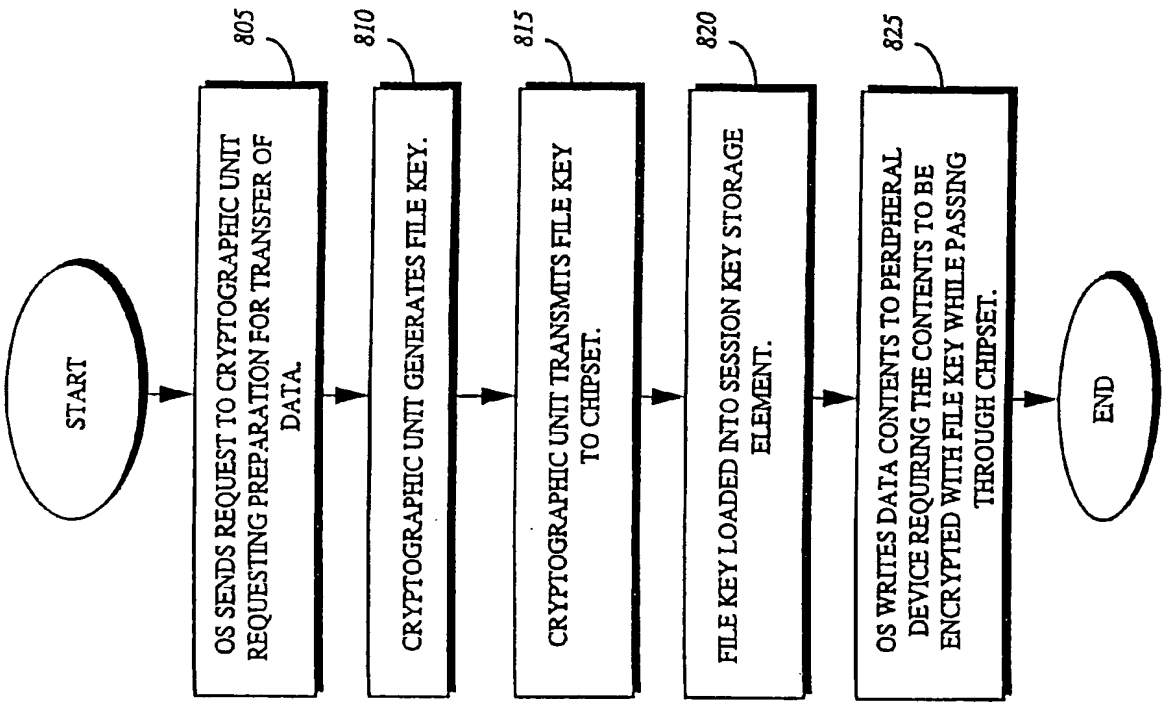

START
805
OS SENDS REQUEST TO CRYPTOGRAPHIC UNIT REQUESTING PREPARATION FOR TRANSFER OF DATA.
810
CRYPTOGRAPHIC UNIT GENERATES FILE KEY.
815
CRYPTOGRAPHIC UNIT TRANSMITS FILE KEY TO CHIPSET.
820
FILE KEY LOADED INTO SESSION KEY STORAGE ELEMENT.
825
OS WRITES DATA CONTENTS TO PERIPHERAL DEVICE REQUIRING THE CONTENTS TO BE ENCRYPTED WITH FILE KEY WHILE PASSING THROUGH CHIPSET.
END

FIG. 8

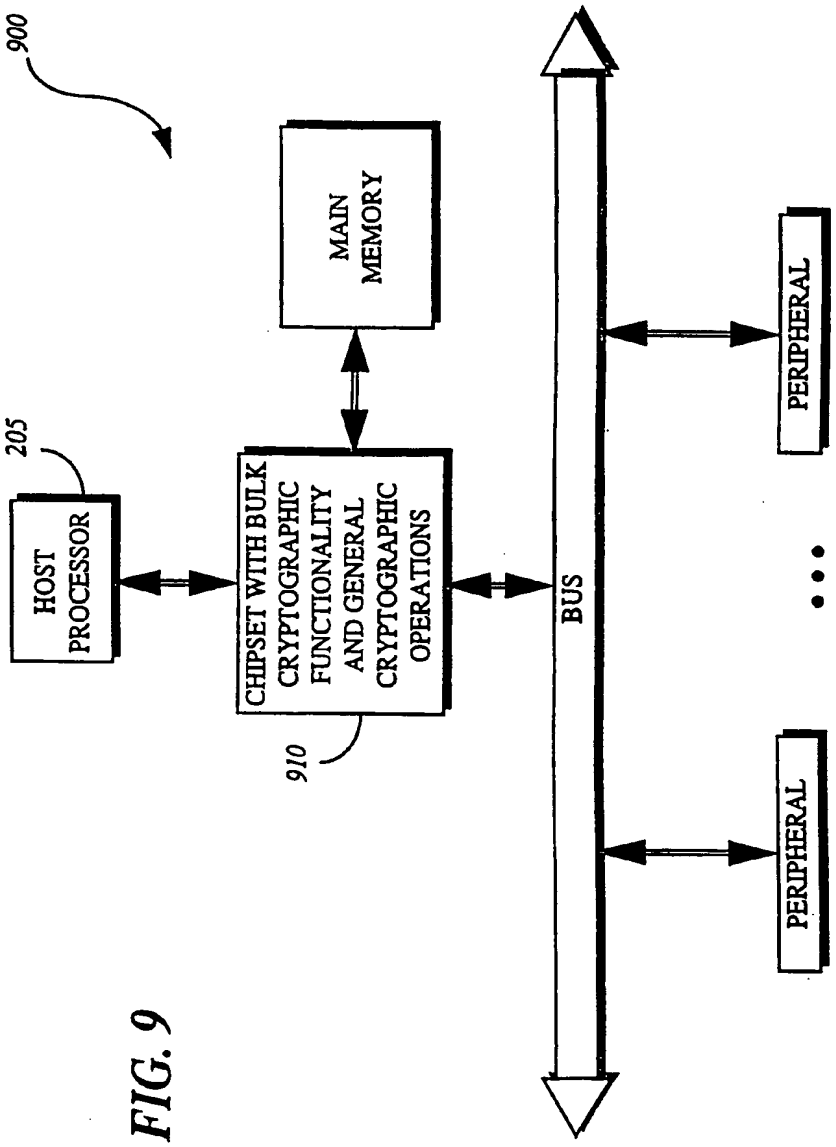
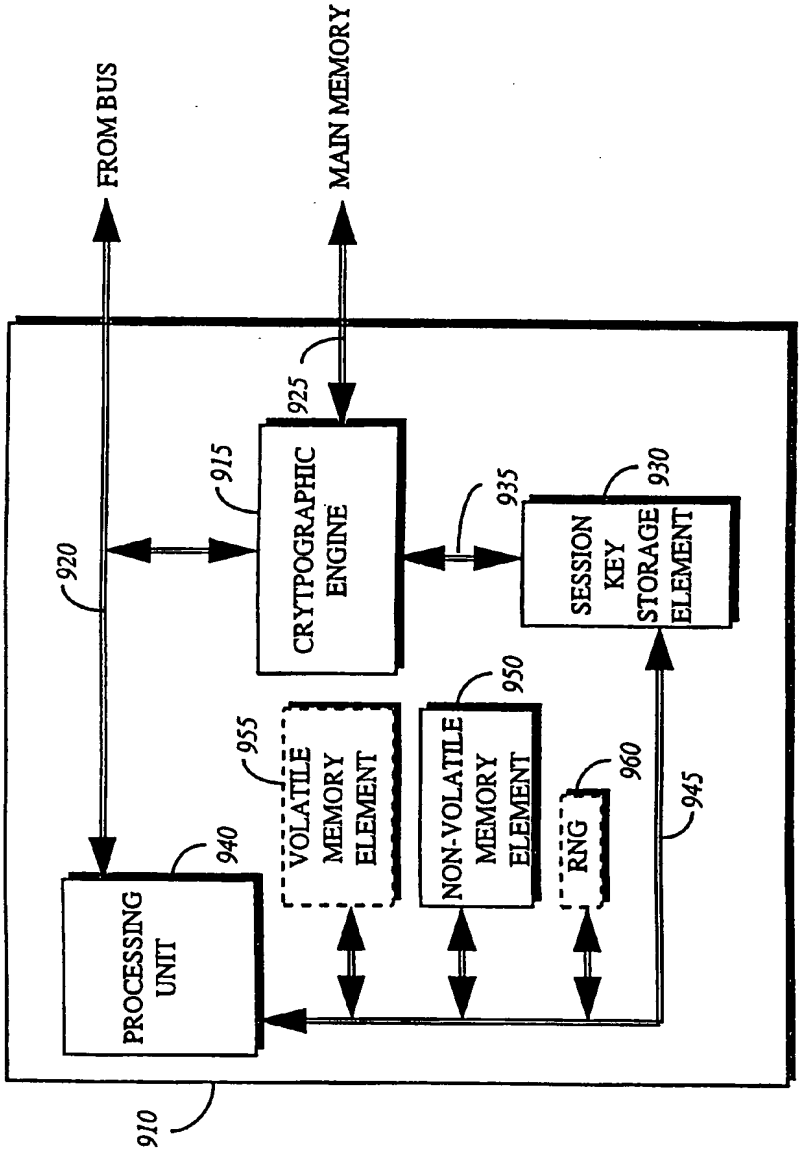

900
MAIN MEMORY
205
HOST PROCESSOR
CHIPSET WITH BULK CRYPTOGRAPHIC FUNCTIONALITY AND GENERAL CRYPTOGRAPHIC OPERATIONS
910
BUS
PERIPHERAL
PERIPHERAL

FIG. 9

FIG. 10


FROM BUS
MAIN MEMORY
925
915
CRYTPOGRAPHIC ENGINE
935
930
SESSION KEY STORAGE ELEMENT
920
950
955
VOLATILE MEMORY ELEMENT
NON-VOLATILE MEMORY ELEMENT
960
RNG
945
940
PROCESSING UNIT
910

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/21900

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00
US CL : 380/49
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/49,4,9,21,23,25,30,44,46,59

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	ZOLLVER. T. As Good As Gold-Telecom Report International. 1995. Vol. 18. No. 4. Siemens AG, Munich, Germany.	1-31

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
19 MARCH 1998	23 APR 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer BERNARR EARL GREGORY Telephone No. (703) 306-4153

Form PCT/ISA/210 (second sheet)(July 1992)*